U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer | NNSA National Nuclear Security Administration

DOE Joint ICAM Program - Unclass & Secret Fabrics

GSA Federal ICAM Day, 16 April 2014
Mr. Frank Husson & Mr. Rich Tannich

Unclassified

Agenda

- Unclassified Initiative
  - Mr. Frank Husson will share DOE’s vision of OneID, which will deliver a set of identity and access management services in YOURcloud, DOE's hybrid community cloud environment.
- Secret Fabric Initiative
  - Mr. Rich Tannich will share the successes that have prepared DOE to implement PKI tokens and how the OneID efforts will be leveraged on the Secret Fabric.

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer | NNSA National Nuclear Security Administration

DOE ICAM Initiative

Enabled through oneID

Mr. Frank Husson
DOE ICAM Agency Lead Official
Office of the Chief Information Officer
Department of Energy
Frank.Husson@hq.doe.gov

OneID at-a-glance

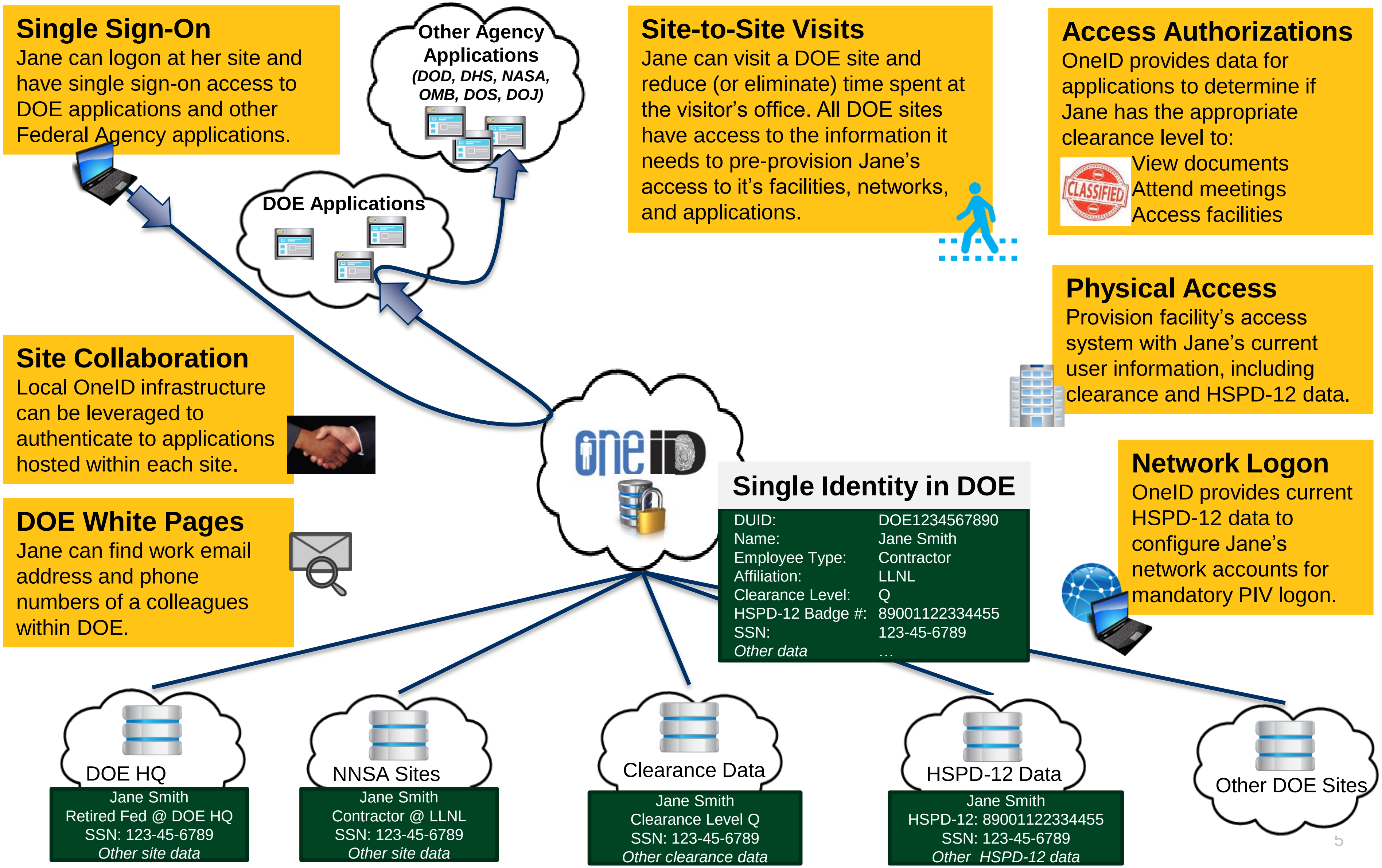
oneID

OneID is an architectural solution being driven by DOE and NNSA to streamline business processes and strengthen authentication capabilities associated with both physical and logical access.

OneID federates the management of identity data, leaving the oversight functions of commissioning and decommissioning cyber access to the owners or hosts of those identities.

Owner:	DOE Associate CIO (ACIO) for Energy IT Services (EITS/IM-60)
Developer:	Lawrence Livermore National Laboratory (LLNL)
Status:	Release 1.0 of OneID Deployed within YOURcloud Enclave
	Initial Operational Capability Targeted for Q2FY14

Value of OneID to End Users



Single Sign-On

Jane can logon at her site and have single sign-on access to DOE applications and other Federal Agency applications.

Site-to-Site Visits

Jane can visit a DOE site and reduce (or eliminate) time spent at the visitor's office. All DOE sites have access to the information it needs to pre-provision Jane's access to it's facilities, networks, and applications.

Access Authorizations

OneID provides data for applications to determine if Jane has the appropriate clearance level to:

View documents
Attend meetings
Access facilities

Physical Access

Provision facility's access system with Jane's current user information, including clearance and HSPD-12 data.

Site Collaboration

Local OneID infrastructure can be leveraged to authenticate to applications hosted within each site.

DOE White Pages

Jane can find work email address and phone numbers of a colleagues within DOE.

Single Identity in DOE

DUID:	DOE1234567890
Name:	Jane Smith
Employee Type:	Contractor
Affiliation:	LLNL
Clearance Level:	Q
HSPD-12 Badge #:	89001122334455
SSN:	123-45-6789
Other data	…

Network Logon

OneID provides current HSPD-12 data to configure Jane's network accounts for mandatory PIV logon.

DOE HQ
Jane Smith
Retired Fed @ DOE HQ
SSN: 123-45-6789
Other site data

NNSA Sites
Jane Smith
Contractor @ LLNL
SSN: 123-45-6789
Other site data

Clearance Data
Jane Smith
Clearance Level Q
SSN: 123-45-6789
Other clearance data

HSPD-12 Data
Jane Smith
HSPD-12: 89001122334455
SSN: 123-45-6789
Other HSPD-12 data

Other DOE Sites

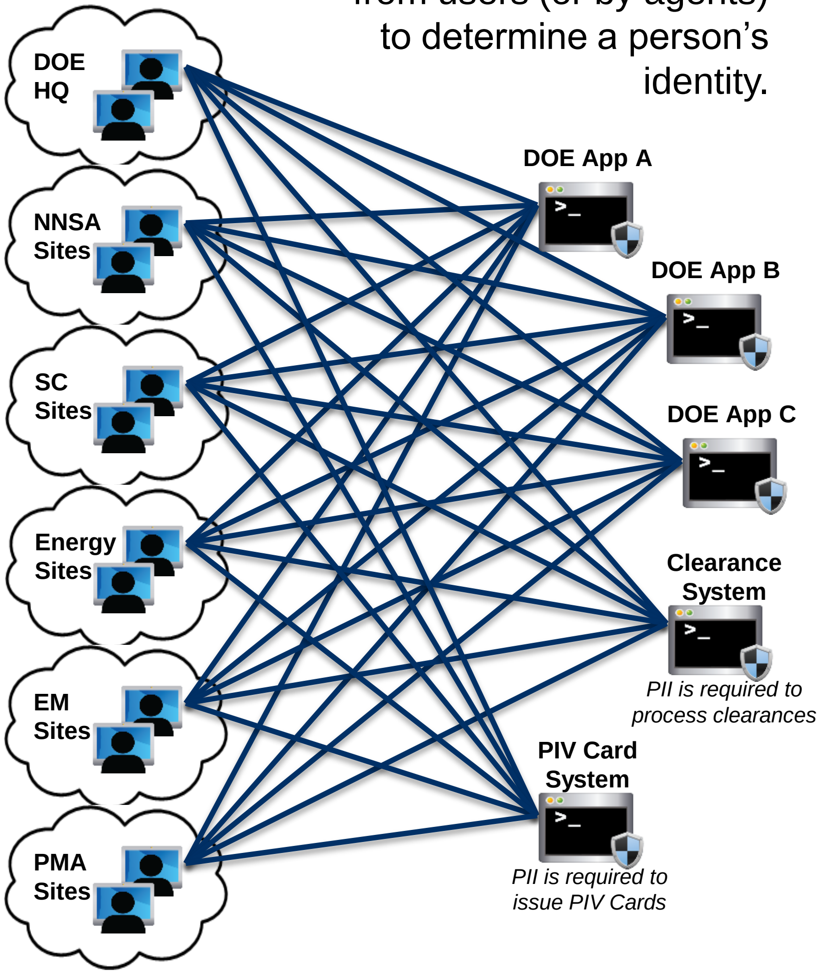
U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer | NNSA National Nuclear Security Administration

Protecting PII with OneID

Control and Secure Exposure of PII

Current State

Applications obtain PII from users (or by agents) to determine a person's identity.



DOE HQ

NNSA Sites

SC Sites

Energy Sites

EM Sites

PMA Sites

DOE App A

DOE App B

DOE App C

Clearance System

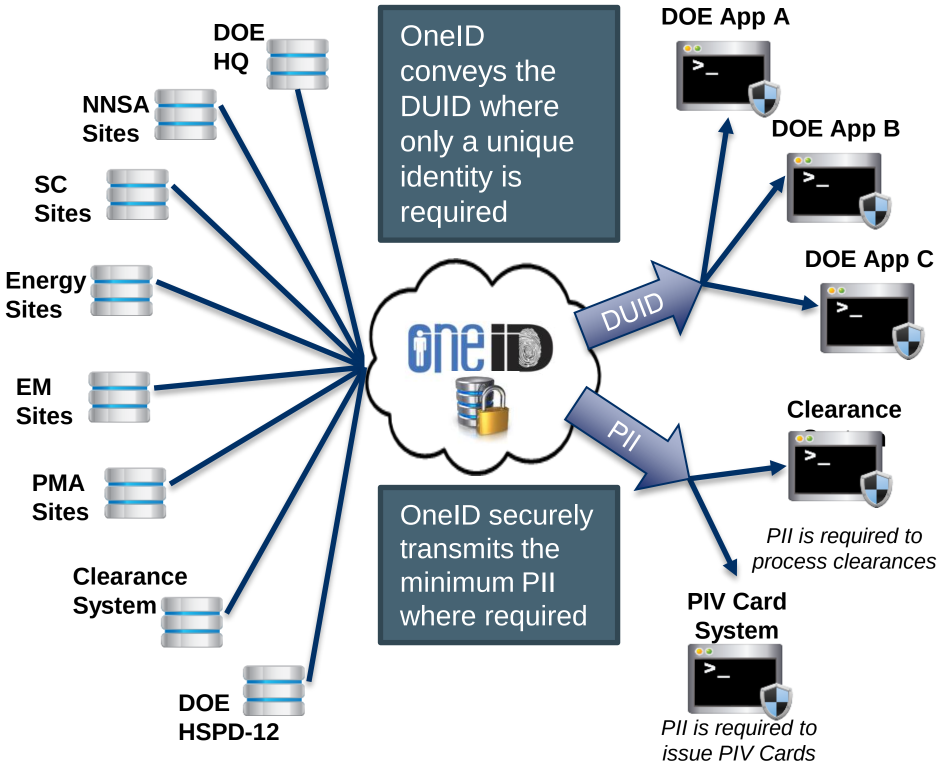
PII is required to process clearances

PIV Card System

PII is required to issue PIV Cards

Target State with OneID

OneID correlates PII from authoritative systems *("sources of truth")* on a private network to establish a person's DOE Unique Identity (i.e., DUID).



DOE HQ

NNSA Sites

SC Sites

Energy Sites

EM Sites

PMA Sites

Clearance System

DOE HSPD-12

OneID conveys the DUID where only a unique identity is required

DUID

PII

OneID securely transmits the minimum PII where required

DOE App A

DOE App B

DOE App C

Clearance

PII is required to process clearances

PIV Card System

PII is required to issue PIV Cards

Summary

The end goal for OneID and ICAM is to extend OneID capabilities enterprise-wide and leverage capabilities on the secret fabric, where appropriate. OneID will:

- Reduce the number of connections transmitting PII between application and users
- Eliminate the need to leverage PII at the application tier for most DOE/NNSA applications
- Improve Security by rapidly de-provisioning access to all supported applications
- Enable a bring-your-own-credential model for DOE sites, labs, and plants that is extensible and will accommodate future needs of DOE

Path Forward

- Complete NNSA site integration
- Finalize scope and project plan for release 2.0
- Develop consensus on multi-year OneID Roadmap
  - Proposal for Physical Access
  - Proposal for classified (secret fabric) adoption
  - Proposal for DOE adoption FY14-15
- Briefing and Proposal for FY16 and beyond (budget planning)

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer | NNSA National Nuclear Security Administration

Partnership on the National Secret Fabric

Mr. Rich Tannich
DOE Secret Fabric ICAM Program Manager
Office of the Chief Information Officer
National Nuclear Security Administration
Rich.Tannich@nnsa.doe.gov

ICAM Includes

- DOE considers ICAM to represent the intersection of digital identities, credentials and access control into one comprehensive approach that is focused on delivering greater convenience and improved security and privacy protection, with less effort and at a lower cost.
- ICAM includes:

Digital Identity
Credentialing
Privilege Management
Authentication

Authorization / Access
Federation
Cryptography
Auditing / Reporting

National Partnership

- Began negotiating with DSAWG for MOU between DOE and DoD (2010)
- Built the ESN–SIPRNet Gateway to DOD (2011)
- Established the Computer Network Defense Service Provider (CNDSP) (2011)
- Built the NNSA Secret Network (NSN) and migrated 11 dedicated Point-to-Point circuits from the labs/plants to SIPRNet (2012)
- Built the DOE Cyber Command Readiness Inspection (CCRI) (2013)
- Joined CNSS and became part of the DISA PKI Common Service Provider (CSP) with 17,000 users on the Secret Fabric (2013)
- Established the CSP Governance Board (2013)
- Building PKI to reach IOC with 10% of population issued tokens for network authentication (December 2014)
- Working with SafeNet and NSA to approve domain-aware token (2014)
- Establishing Joint DOE ICAM program with Unclassified initiative to integrate OneID for users on both fabrics (2014)
- Re-engineering ESN to accommodate OneID (2014)

ESN Re-engineering

- ESN has a mature Identity and Access Management solution in place since 2009.
- ESN products are end of life, costly to maintain and not gracefully modified to support ICAM requirements.
- Changing landscape of DOE Secret environment and Federal Secret fabric requires a more flexible, modular approach to identity management.
- Plan to leverage the OneID Attribute Exchange Service (AES) to incorporate into the new classified IdM solution.
- Data will be moved from AES into the classified environment via a data diode, where it will be supplemented with additional user attributes available only in the Secret environment, including:
    - Classified e-mail address
    - Access Authorizations for Sigma categories
    - Need to Know (NTK) group membership
- New ESN design, including software and tools, will be used in other Secret environments, such as NSN.

National Alignment

- **DOE Joint ICAM initiative is closely aligned with the requirements and milestones from both:**
  - **Committee on National Security Systems (CNSS)**
  - **Information Sharing and Access Interagency Policy Committee (ISA IPC)**
- **DOE personnel strategically embedded in leadership roles in both National organizations to influence the direction of the Federal ICAM (FICAM) initiative.**

Thank You

Mr. Frank Husson
DOE ICAM Agency Lead Official
Office of the Chief Information Officer
Department of Energy
Frank.Husson@hq.doe.gov

Mr. Rich Tannich
DOE Secret Fabric ICAM Program Manager
Office of the Chief Information Officer
National Nuclear Security Administration
Rich.Tannich@nnsa.doe.gov

Powered by EAS

icam

YOUR KEY TO USDA

ICAM Day

USDA ICAM Program

USDA

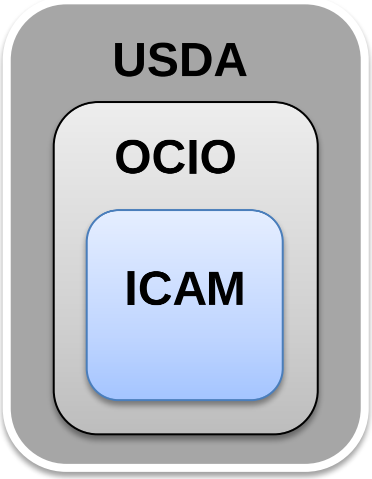
April 16, 2014

USDA ICAM Program

icam
YOUR KEY TO USDA
Powered by EAS

- Background
- Services
- Statistics
- Logical architecture
- Roadmap

ICAM Organization in USDA

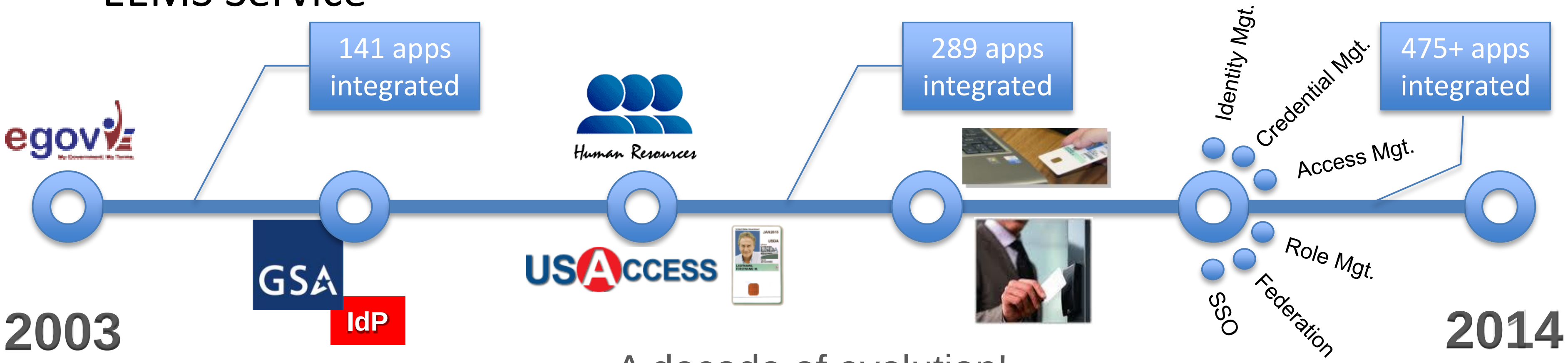


- The role of the USDA OCIO’s office is to provide technical solutions for the 7 mission areas to allow bureaus to focus on their respective mission.

- ICAM responsibilities are distributed in USDA:
  - **Departmental Management - Office of Homeland Security and Emergency Coordination** is responsible for PIV issuance and physical access control (e.g. facilities, buildings)
  - **Office of the CIO – ICAM Program** is responsible for enterprise identity management, single sign-on access to USDA web-based and mobile applications, digital signature, enterprise role based authorization, and logical access control guidance
  - **Office of the CFO – National Finance Center** is responsible for managing the employee and contractor human resource records.

USDA ICAM History

- Went live with “eAuthentication” as a highly-available enterprise-wide service for web single sign-on in 2003 as part of the eGov initiative
- Approved as one of GSA’s eAuthentication identity providers (IdP) for external federated identities in 2006
- Integrated HR and HSPD-12 systems to automate and streamline identity management and PIV card issuance in 2007
- Enabled LincPass (PIV) authentication for LACS in 2010
- Expanded the ICAM program to manage the full identity lifecycle, including on\off-boarding, provisioning, and RBAC in 2011 with the EEMS Service



2003

141 apps integrated

GSA IdP

Human Resources

USAccess

289 apps integrated

Identity Mgt.

Credential Mgt.

Access Mgt.

Role Mgt.

Federation

SSO

475+ apps integrated

2014

A decade of evolution!

USDA ICAM Services

- Provides identity lifecycle management & access control to the entire USDA enterprise (29 agencies\bureaus)
- Identity Management:
  - On-board & off-board employees
  - Automated Provisioning of Accounts and Permissions
  - Entitlement Management
- Access Management:
  - Web Single Sign-On (475+ Applications, 4 million logons per month)
  - PIV-Enablement
  - Federated Authentication with External Partners
- Shared Service offering supports non-USDA Federal Agencies

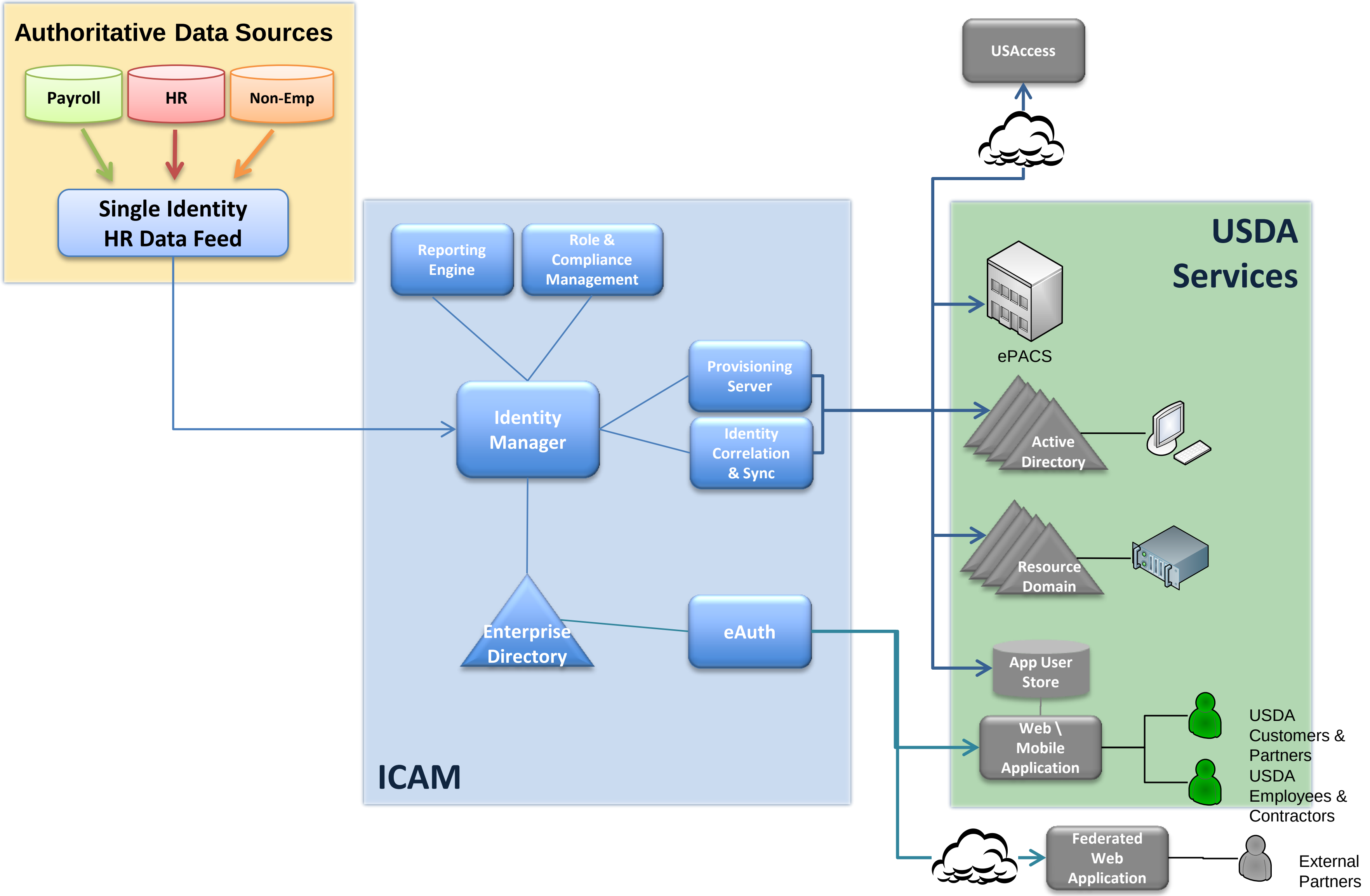
USDA ICAM Statistics*

- ICAM supports USDA and its sub-agencies (e.g., Forest Service & Animal, Plant, Health Inspection Service)
- ICAM partners with other federal agencies (e.g., HHS, DOJ, NIH, DOI, OPM)
- ICAM is federated with external entities (e.g., SalesForce.com, GovTrip, eOPF)

- 642,312 total accounts (internal USDA & public citizen accounts in eAuthentication)
- 104,357 active internal USDA accounts
- 475+ applications (internal and public-facing) protected with eAuthentication
- 4,806,940 authentication events (logins) per month
- 198,728,073 single sign-on transactions per month

**Statistics as of 4/08/2014*

ICAM Logical Architecture



Roadmap

- ICAM as a Service
  - Provides federated identity, credential, and access management services for Federal Agency systems.
- Federation Enhancements
  - Interoperability with federal agency partners
  - Acceptance of externally issued credentials for citizens\customers
  - Identity data\attribute exchange

- PIV-Derived Credentials
- Enhanced mobile computing integration
- Expand Identity Management services
  - Role and Compliance Management

USDA ICAM Team

- Adam Zeimet, Chief Architect (Acting Director)
  - 970-295-5678
  - Adam.Zeimet@ocio.usda.gov
- Shari Erickson, ICAM Deputy Director
  - 970-295-5128
  - Shari.Erickson@ocio.usda.gov
- Jake Guzman, ISSO
  - 970-295-5150
  - Jacob.Guzman@ocio.usda.gov

Powered by EAS

icam

YOUR KEY TO USDA

ICAM Day

Realizing the Benefits of ICAM

Ken Calabrese

Associate Director, Office of Security and Strategic Information and HSPD-12 Program Manager

Department of Health and Human Services

April 2014

Status of HSPD-12 at HHS

- Over 70% of non-privileged staff required to use PIV card to access network
- Implementation of Alternate Logon Token (ALT) card has been initiated for privileged accounts
  - Non-identity card interoperable with PIV
- PACS integrated with LACS
- Implementation of Restricted Local Access (RLA) for short term staff and foreign nationals not qualifying for PIV
  - Identity card interoperable with PIV
- Simplified Signon provides access to HHS and line of business applications using PIV

Benefits of ICAM – User Perspective

- Simplified access to infrequently used applications
- Common credential to access systems
  - Network
  - Remote VPN
  - Applications
- Substantially reduced help desk calls for password resets
- Digital signature
- Simplified access to facilities
  - Permanent duty station
  - Authorized facilities HHS-wide

Benefits of ICAM – Security

- Strong authentication for direct and remote access to networks and applications
  - ICAM caused HHS to review level of access and implement appropriate credential
- Assurance of background investigation
  - HSPD-12 caused HHS to assure all staff have NACI
- Foreign Nationals
  - HSPD-12 caused HHS to address challenges with background investigations for foreign nationals
- Integration of PACS and LACS assures physical access immediately revoked

Benefits of ICAM – Security (Continued)

- Common identity card across HHS/Federal Government
  - HHS would not have mandated single card itself
- Complete database of all staff
  - Currently most complete people repository in HHS
- HHS-wide unique identifier facilities elimination of social security numbers as unique identifier in applications
- Last four digits of unique identifier used as security code to access VISA card account supporting subsidized transit in place of last four of social security number
- Unique identifier allows correlation between systems such as HR and Active Directory